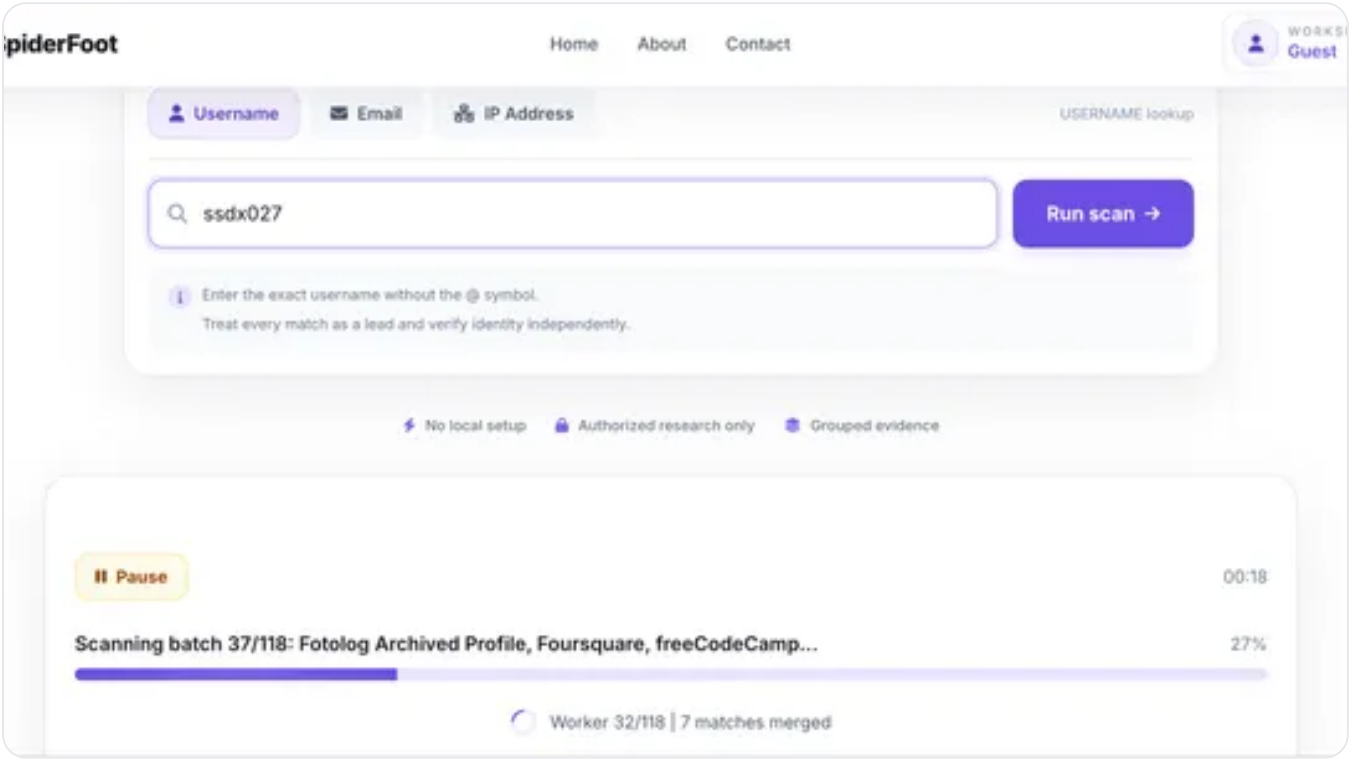
SpiderFoot OSINT Tool

Free online OSINT for usernames, email addresses, and IPs.



About

SpiderFoot OSINT Tool is a free online OSINT tool for investigating usernames, email addresses, IP addresses, and public information. It gives you a browser-based way to run targeted public-source checks, review grouped evidence, and follow scan progress without installing anything locally.

What is SpiderFoot OSINT Tool

SpiderFoot OSINT Tool is a web-based open-source intelligence workspace that helps you investigate public identifiers from a browser. It focuses on three target types shown in the product flow: usernames, email addresses, and IP addresses. The service is built for research workflows where you want visible scan progress, source-backed results

The app's own positioning is narrow and practical: it is designed for public data only, it requires no local installation, and it emphasizes that matches should be treated as leads rather than proof. That makes it more of an OSINT research utility than a general search engine.

Key features

SpiderFoot OSINT Tool centers on a small set of evidence-oriented features:

- **Username discovery**: check a username across public web sources to surface profiles, related accounts, and connected signals.
- **Email exposure search**: review account traces and exposure indicators tied to an email address.
- **IP intelligence**: inspect IP context such as geolocation, ASN, organization, and routing details using Cloudflare-powered intelligence.
- **Grouped results**: findings are organized into a single workspace instead of scattered across separate tabs or tools.
- **Transparent scan state**: the interface shows active scanning and can also return no matches or incomplete results.
- **Browser-based access**: you can use it online without local setup or software installation.
- **Saved history**: the workspace mentions saved history, which can help you revisit prior lookups.

These capabilities make it useful when you need a lightweight public-record lookup tool rather than a full incident response platform.

How to use it

1. Open the web app in your browser and choose the type of target you want to investigate: username, email, or IP address.
2. Enter the identifier exactly as requested. For username lookups, the product instructs you to leave off the @ symbol.
3. Run the scan and wait while public sources respond. The interface shows scanning

Review the grouped evidence that comes back. Look for source context, patterns, and related signals rather than treating one result as definitive.

Verify any important match independently before drawing conclusions.

If the scan returns no public matches or cannot complete, refine the input, check spelling, or try another identifier.

A practical workflow is to start with one identifier, read the result sources carefully, and keep notes on what is confirmed versus what still needs verification.

Who it is for

SpiderFoot OSINT Tool is aimed at people who need structured public-source research with minimal setup. Common use cases include:

security researchers who want quick OSINT leads

investigators who need browser-based identity or footprint checks

developers or analysts who want IP context without a separate local install

users comparing public profile signals across usernames and emails

anyone who prefers a guided research workspace over manual source-hopping

It is best suited to users who understand that OSINT output is directional. The app surfaces evidence, but it does not resolve identity on its own.

What to know before you use it

This service has some important limits, and those limits matter for how you interpret results.

It is built for **public data only**; it is not a private-data access tool.

It does **not** confirm identity automatically. The site explicitly says to treat every match as a lead and verify it yourself.

Results can be incomplete. The interface may show that a scan could not be completed or that no public matches were found.

Username searches require the exact value and should be entered without the @ symbol.

The IP lookup uses Cloudflare-powered intelligence, but that still provides context, not guaranteed attribution.

If you need authoritative records, use the original platform, the official account owner, or another primary source instead of relying on a scan result alone.

The app mentions responsible use and authorized research only, so it is not intended for misuse or intrusive activity.

SpiderFoot OSINT Tool is most valuable when you need a fast, browser-first way to collect public leads, then verify them elsewhere. Use it as an investigation aid, not as the final source of truth, and always confirm important findings before acting on them.

FAQ

Is SpiderFoot OSINT Tool free to use?

What can I search with it?

Does it work on mobile apps or only in a browser?

How should I enter a username search?

Can I rely on the results as proof?

Sponsored

Belay – Awa... Featured

Developer Tools

Stays awake while your agents work.

Free # Developer Tools

View ↗

Partly Featured

Finance

Partly is a mobile app that lets friends quickly scan receipts, split any bill fairl...

Free # Finance

View ↗

Visit website ↗

spiderfoot-osint-tool

Pricing	Free
Category	Developer Tools
Platform	Web
Launched	Aug 2026
Updated	today
Verified	yesterday

TAGS

osint # investigation # username lookup # email search # browser-based # ip intelligence # public data

SpiderFoot OSINT Tool